

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-182289

(43)Date of publication of application : 21.07.1995

(51)Int.Cl. G06F 15/00
G06F 15/00

(21)Application number : 05-327646

(71)Applicant : SEIKO EPSON CORP

(22)Date of filing : 24.12.1993

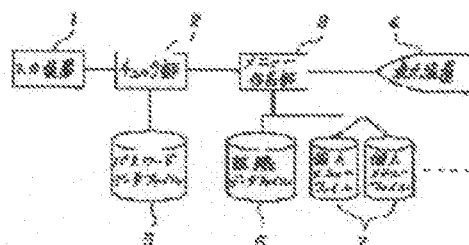
(72)Inventor : MATSUZAWA YOSHIHIKO

(54) METHOD AND DEVICE FOR SECURITY MANAGEMENT

(57)Abstract:

PURPOSE: To improve the maintenance of an information system and the safety of secrecy even when increment in the number of users or the number of sections or personnel changes are generated in security management.

CONSTITUTION: This security managing device is constituted of an input device 1 for inputting a log-in name or the like, a checking part 2 for identifying a valid user, a menu preparing part 3 for preparing a menu, a display device 4 for displaying the menu, a password data file 5 for storing user information, an organization data file 6 storing the hierarchical information, employees' codes, etc., of an organization, and a personal menu data file 7 storing the menu information of each user. In the case of preparing a personal menu for an optional user, information identifying the user is inputted from an input device 1, the user is checked by a checking part 2 and a menu preparing part 3 retrieves a section to which a person in charge of security management belongs and a supervisor from an organization data file 6, applies restriction based upon a personal menu file 7 for the supervisor and newly prepares a personal menu file 7.



LEGAL STATUS

[Date of request for examination] 16.11.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3536329

[Date of registration] 26.03.2004

[Number of appeal against examiner's decision of rejection]

(18) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-182289

(43) 公開日 平成7年(1995)7月21日

(51) Int. Cl. ⁵	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 D	7 4 5 9 - 5 L		
	3 1 0 S	7 4 5 9 - 5 L		

審査請求 未確定 請求項の数 5 O L (全 8 頁)

(21) 出願番号 特願平5-327646

(22) 出願日 平成5年(1993)12月24日

(71) 出願人 000092369

セイコーエプソン株式会社

東京都新宿区西新宿2丁目4番1号

(72) 発明者 松沢 義彦

長野県諏訪市大和3丁目3番5号セイコー

エプソン株式会社内

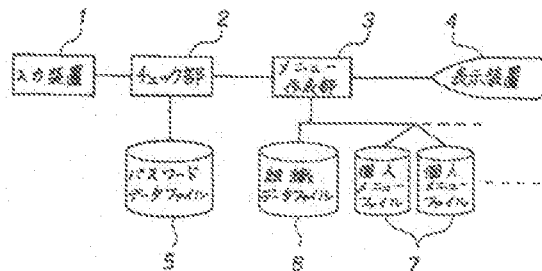
(74) 代理人 弁理士 鈴木 喜三郎 (外1名)

(54) 【発明の名称】 セキュリティ管理方法およびセキュリティ管理装置

(57) 【要約】

【目的】 セキュリティ管理において利用者数、部署数の増加、人事異動が生じた場合でも情報システムの保守性と、機密安全性を高めることを目的とする。

【構成】 ログイン名等を入力する入力装置1と、正当な利用者を識別するチェック部2と、メニューを作成するメニュー作成部3と、メニューを表示する表示装置4と、利用者情報が格納されたパスワードデータファイル5と、組織の階層情報、社員コード等が格納された組織データファイル6と、利用者毎のメニュー情報が格納された個人メニューデータファイル7から構成され、任意の利用者の個人メニューを作成するときは入力装置1より前記利用者を識別する情報を入力し、前記利用者をチェック部2でチェックした後、メニュー作成部3で組織データファイル6により該当する担当者の所属部署、管理者を検索し管理者の個人メニューファイル7を基に制限を加え、新たに個人メニューファイル7を作成する。



【特許請求の範囲】

【請求項1】 用意された処理またはデータ選択メニューから利用者が必要とする処理またはデータのみを選択し、利用者独自のメニューを作成するメニュー作成機能と、情報処理システムの利用者を特定するための利用者識別機能と、利用者が所属する組織データの管理機能を備えたセキュリティ管理方法において、

メニュー作成機能により任意の利用者Aの処理またはデータ選択メニューを作成するとき、前記組織データを基に前記利用者Aの所属する部署または組織の上位者を検索し、部署または上位者が使用している処理およびデータ選択メニューの範囲から作成することを特徴とするセキュリティ管理方法。

【請求項2】 上記請求項1記載のセキュリティ管理方法であって、前記利用者Aが処理およびデータ選択メニューを利用するときは、前記利用者識別機能によって識別された前記利用者Aは前記利用者A以外が作成した処理およびデータ選択メニューしか利用できないことを特徴とするセキュリティ管理方法。

【請求項3】 上記請求項1記載のセキュリティ管理方法であって、前記利用者Aがメニュー作成機能により前記利用者Aの処理またはデータ選択メニューを作成するとき、前記組織データを基に前記利用者Aの所属する部署または組織の上位者を検索し、部署または上位者が使用している処理およびデータ選択メニューの範囲から限定して定義した処理およびデータ選択メニューから作成することを特徴とするセキュリティ管理方法。

【請求項4】 上記請求項1記載のセキュリティ管理方法であって、前記利用者Aの組織上の所属が変更となったとき、前記組織データを変更する処理の中で、既に作成された前記利用者Aの処理またはデータ選択メニューを無効とすることを特徴としたセキュリティ管理方法。

【請求項5】 用意された処理またはデータ選択メニューから利用者が必要とする処理またはデータのみを選択し、利用者独自のメニューを作成するメニュー作成手段と、情報処理システムの利用者を特定するための利用者識別手段と、利用者が所属する組織データの管理手段を備えたセキュリティ管理装置において、

メニュー作成手段により任意の利用者Aの処理またはデータ選択メニューを作成するとき、組織データを基に前記利用者Aの所属する部署または組織の上位者を検索し、部署または上位者が使用している処理およびデータ選択メニューの範囲から作成する手段を有することを特徴とするセキュリティ管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は情報処理システムにおけるセキュリティ管理方法および装置に関する。

【0002】

【従来の技術】 情報処理システムにおいてセキュリティ

管理を行う方法として、特公平の3-27224号公報にあるようにパスワードによる利用者の識別と、利用者毎の利用可能なメニューおよびデータ範囲の設定が一般的である。さらに、選んだ方法として企業における利用を主眼とした場合は、特開平の3-246742号公報のように、利用者・部門別の画面利用情報をデータとして管理し、重要メニュー、サブメニューの様に階層化して利用者名、パスワードと一致した場合のみ利用可能とすることにより機密性を高める方法がある。このような現在のセキュリティ管理を利用しても企業内の組織体系に合わせた設定を行うことは可能であり、情報処理システムを管理する部署が利用者の身分あるいは部門、課などを考慮してメニューの設定を行っている。

【0003】

【発明が解決しようとする課題】 しかし従来技術では利用者数が少ない場合には問題ないが、従業員一人一人に上記のパスワード、メニューを設定した場合や、組織の数が増加した場合、情報処理システム管理部門の作業負担が大幅に増えることになる。また情報処理システム管理部門は、組織内の各部署がどのような処理やデータを利用するか詳しく知らないために、必要以上に許可範囲を狭くしたり、逆に本来許可されるべきでない情報も許可されるといった弊害もでてくる。企業では組織の変更や人員の異動は頻繁に行われるが、人事異動などが発生した場合は個人毎の許可範囲が変わるので改めてメニューやパスワードの設定を行なう必要があり、保守にも手間がかかるといった問題がある。またその対応が遅かったり忘れた場合は本来は禁止されるべき元の部署の情報がアクセスでき、新しい部署での情報にアクセスができないといった問題が起きる。

【0004】 本発明は、このようなセキュリティ管理と企業組織との不整合を無くして、企業組織に合った形でセキュリティ管理ができ、設定および変更を容易にすることにより、情報システム部門の作業負担を軽減し、かつ機密安全性を高めることを目的とする。

【0005】

【課題を解決するための手段】 本発明のセキュリティ管理方法は、用意された処理またはデータ選択メニューから利用者が必要とする処理またはデータのみを選択し、利用者独自のメニューを作成するメニュー作成機能と、情報処理システムの利用者を特定するための利用者識別機能と、利用者が所属する組織データの管理機能を備えたセキュリティ管理方法において、メニュー作成機能により任意の利用者Aの処理またはデータ選択メニューを作成するとき、前記組織データを基に前記利用者Aの所属する部署または組織の上位者を検索し、部署または上位者が使用している処理およびデータ選択メニューの範囲から作成することを特徴とする。

【0006】 また、前記利用者Aが処理およびデータ選択メニューを利用するときは、前記利用者識別機能によ

3

って識別された前記利用者Aは前記利用者A以外が作成した処理およびデータ選択メニューしか利用できないことを特徴とする。

【0007】また、前記利用者Aがメニュー作成機能により前記利用者Aの処理またはデータ選択メニューを作成するとき、前記組織データを基に前記利用者Aの所属する部署または組織の上位者を検索し、部署または上位者が使用している処理およびデータ選択メニューの範囲から限定して定義した処理およびデータ選択メニューから作成することを特徴とする。

【0008】また、前記利用者Aの組織上の所属が変更となったとき、前記組織データを変更する処理の中で、既に作成された前記利用者Aの処理またはデータ選択メニューを無効とすることを特徴とする。

【0009】本発明のセキュリティ管理装置は、用意された処理またはデータ選択メニューから利用者が必要とする処理またはデータのみを選択し利用者独自のメニューを作成するメニュー作成手段と、情報処理システムの利用者を特定するための利用者識別手段と、利用者が所属する組織データの管理手段を備えたセキュリティ管理装置において、メニュー作成手段により任意の利用者Aの処理またはデータ選択メニューを作成するとき、組織データを基に前記利用者Aの所属する部署または組織の上位者を検索し、部署または上位者が使用している処理およびデータ選択メニューの範囲から作成する手段を有することを特徴とする。

【0010】

【作用】情報システムで用意されたメニューの中から利用者が必要とするメニューを選択して利用者独自のメニューを作成するメニュー作成機能と、利用者を特定するための利用者識別機能と、利用者が所属する組織データの管理機能を備えているとき、メニュー作成機能により特定の利用者のメニューを作成するときには組織データを検索して組織の上位者を識別し、その上位者または部署が使用しているメニューの範囲から限定して作成することによりセキュリティ管理を向上する。

【0011】

【実施例】本発明の実施例を図を用いて説明する。図1は本発明のブロック図である。ログイン名、パスワード、社員コード等を入力するための入力装置1と、入力されたログイン名、パスワード、社員コード等から正当な利用者かどうかをチェックするチェック部2と、表示メニューを作成するためのメニュー作成部3と、作成したメニューを表示するためのCRT等の表示装置4から構成され、さらにチェック部2で正当な利用者がチェックを行うための正当な利用者の情報が格納されたパスワードデータファイル5と、組織の階層情報、社員コード等が格納された組織データファイル6と、利用者の個人毎のメニューの情報が格納された個人メニューデータファイル7から構成されている。5、6、7はそれぞれ補

助記憶装置に格納されている。

【0012】図10は本実施例の概念を実際のメニュー例として示した図である。情報システムの機能の全メニューが101であり、管理レベルは全社、トップ管理者が利用できるメニューである。全メニュー101より財務会計部分のメニューのみを作成したメニューが102であり、管理レベルは部、管理する部門は財務部で、財務部の部門管理者が使用するメニューである。さらに管理レベルが部門のメニューから管理レベルが課単位のメニューを経て、管理レベルが担当者のメニュー103を作成している。これらの過程で組織データファイル6に含まれる会社の組織構造を参照して下位のメニューを作成している。

【0013】図2はパスワードデータファイル6の例であり、全ての利用者を識別するための情報が21に格納されている。利用者を識別するためのログイン名、利用者を特定するための利用者のみが知るパスワード、社内で従業員に一意に付けられた利用者の社員コード、利用者毎のメニューの情報が格納された個人メニューファイル7のファイル名から構成されている。

【0014】図3は個人メニューファイル7の例であり、利用者一人一人に31に示す情報が格納されたファイルがある。一つ一つのメニュー項目を識別するためのメニューコード、メニューを表示装置4に表示するときに表示するかどうかを示す表示フラグ、メニュー作成部3で表示データを作成する時に使用するメニューの表示名、利用者が情報システムを使用して処理を起動するとき、メニュー項目と処理プログラムを結び付けるための起動プログラム名から構成されている。

【0015】図4は組織データファイル6の例であり、会社の組織構造を格納したファイル41である。企業内で組織の階層に従って部署毎に一意に付けられた部署コードと部署名、その部署の管理者（例えば課長）の社員コード、その部署の所属員の社員コード（複数）から構成され、社員コードから所属部署が検索できるようになっている。また部署コードにより上位部署名も分かるように構成されている。

【0016】次に本実施例を図5のフローチャートを用いて説明する。図5は個人メニューを利用する担当者以外の人が個人メニューファイルを作成する時の処理フローチャートである。入力装置1より作成する担当者の社員コードを入力する(ST1)と、社員コードが正当かチェック部2でチェックする。正当であればメニュー作成部3で組織データファイル6を補助記憶装置から読み込む(ST2)。組織データファイル6では社員と所属部署の関係を情報として格納しているので、社員コードを基に所属部署とその部署の管理者を検索する(ST3)。検索の結果から管理者の社員コードが分かるので、パスワードデータファイル6から管理者の個人メニューファイル名を検索し、個人メニューファイル7を読

10

20

30

40

50

み込む(ST4)。メニュー作成部3では、この管理者の個人メニューファイルから表示データを作成し、表示装置4にメニューを表示する(ST5)。

【0017】ST6、ST7、ST8は管理者の個人メニューの中から担当者に表示を許可するかどうかを入力する処理であり、入力装置1から認可、否認可を入力し(ST6)、否認可とするメニュー項目は削除し(ST7N、ST8)。認可するメニュー項目はそのまま残す(ST7Y)。設定項目が終了したら(ST9Y)担当者の個人メニューファイルに書き込む。これにより、管理者の個人メニューファイルから認可するメニュー項目のみで構成された担当者用の個人メニューファイルが作成できる。

【0018】図6は図5のフローチャートの処理に従って担当者用のメニューを作成した例である。経理1課の課長に許可されたメニュー61は、この課長の個人のメニューであり7個のメニュー項目からなる。このメニューから作成され担当者に許可されたメニューが62であり、3個のメニュー項目となっている。このように本実施例によれば、組織上の上位者のメニューから削除して下位者のメニューを作る事ができるので全体メニューから作る場合に比べ少ない操作で担当者のメニューを作成できる。また、経理1課の許可範囲が課長自身のメニューにより制限されているので、経理1課の業務に詳しくない人が設定しても許可範囲の誤りなく個人メニューファイルを作成できる。

【0019】つぎに、担当者が自分のメニューを作成するときの実施例を図7のフローチャートに従って説明する。担当者は入力装置1より自分のログイン名、パスワードを入力すると(ST21)、チェック部2ではパスワードデータファイル5を検索して利用者に登録されているかどうかをチェックする(ST22)。正当な利用者であればメニュー作成部3で、この担当者の個人メニューファイルが作成済みかどうかをチェックし(ST23)。作成済みであればST23Yに行く。未作成であればST23Nに行き、組織データファイル6を読み込む(ST24)。社員コードを基に組織データファイル6から所属部署とその部署の管理者を検索する(ST25)。検索の結果から管理者の社員コードが分かるので、パスワードデータファイル5から管理者の個人メニューファイル名を獲得し、この管理者の個人メニューファイルを担当者の個人メニューファイルにコピーする(ST26)。この情報を基に表示データを作成して表示装置4にメニューを表示する(ST27)。ST28、ST29、ST30では担当者自身が必要と思われるメニュー項目を表示する。しないを入力する。表示する場合は個人メニューファイル31の表示フラグをON(ST31)。表示しない場合はOFF(ST30)とする。メニュー項目の設定が終了(ST32Y)段階で個人メニューファイルを書き込む。これにより、この担

当者の個人メニューファイルが作成される。

【0020】担当者が自分のメニューを作成するのは次の二つの場合が考えられる。一つは上位者(例えば課長)が図5のフローチャートによって作成済みの個人メニューファイルがあるが、担当者がさらに操作性を向上したい場合であり、もう一つは上位者と担当者のセキュリティ管理レベルがほとんど同じ(例えば課内のグループ長と担当者)場合で担当者は未作成の状態から個人メニューを作れば良い。

【0021】図8は作成済みの個人メニューを基に各メニュー項目を編集することによって、見やすく操作性を向上するための操作画面例である。作成済みの個人メニューを表示したウィンドウが81であり、作成済み個人メニューウィンドウ81を階層構造で表示した基メニューウィンドウが83である。これを基に表示、非表示の入力、およびメニュー項目の順番入れ換えなどの操作を行う編集ウィンドウが82である。個人メニューを変更するには、基メニューウィンドウ83の中で設定ボタンをポインティングデバイス例えばマウスでクリックすると、基ウィンドウ83と同じ内容が編集ウィンドウ82に表示される。この編集ウィンドウ82の中で、例えば日常業務のメニュー項目をクリックし、非表示に設定。経営分析のメニュー項目をクリックしメニューの先頭に移動などの操作を行う。その結果が編集ウィンドウ82の様に、先頭に経営分析、経営分析情報設定、帳表作成のメニューとなっている。この編集操作を終了すれば、メニューウィンドウ81は編集ウィンドウ82に従ったメニューになる。

【0022】図9は人事異動にともなって担当者の所属部署が変更になったときの、個人メニューを無効とするフローチャートである。入力装置1から異動者の社員コードを入力する(ST50)。社員コードの正当性をチェック後、社員コードを基にパスワードデータファイル5から個人メニューファイル名を得て、このファイルを削除する(ST51)。次に組織データファイルを読み込んで(ST52)元籍の部署から異動者の社員コードを削除する(ST53)。次に入力装置1から異動先の部署の部署コードを入力し(ST54)。異動先部署に異動者の社員コードを追加する(ST55)。組織データファイルを補助記憶装置に書き込み(ST56)、終了する。これにより組織データを変更するだけで異動した担当者のメニューは削除され、しかもパスワードは残されているので、この後異動者が情報システムを利用しようするとログインは可能であるが元籍の部署のメニューは表示されない。新たなメニューは新しい部署での上位管理者のメニューから作成するので、システム管理部門の手間をかけずに、人事異動に伴うセキュリティ管理が容易にできる。

【0023】さらに、本実施例では管理者の個人メニューファイルを基に下位者の個人メニューファイル7を作

7

成する例を示したが、組織変更によっても管理者自身も人事異動することもある。この場合、一時的に管理者レベルの個人メニューファイルが無くなってしまふ不都合も発生する。これを防ぐには管理者の個人メニューファイルではなく、仮想的な管理者を設定し仮想管理者のパスワード、個人メニューファイルを作成して置けばよい。さらに仮想管理者のログイン名を部署コードと一致させれば、即ち部署単位でメニューが作成できることになる。パスワードデータファイルの中に部署コードをログイン名として設定すれば、図5のフローチャートにより、部署単位でメニューが作成できる。担当者の個人メニューを仮想管理者(部門)の個人メニューから作成すれば、管理者個人のメニューと、組織上のメニューと分離することができる。

【0024】また本実施例ではログイン名と社員コードを別のものとして説明したが、共に情報システム内では一意であるので、ログイン名に社員コードを使用すれば、パスワードデータファイルの容量が少なくなり、情報システム管理部門の作業負担も少なくなる。

【0025】また、本実施例では企業内の組織を例に説明したが、関連会社を含めた組織にも適用できる。例えば、本社と複数の関連会社がある場合、関連会社を一部門に位置付けて組織データファイルに組み込めば、関連会社の担当者もセキュリティ管理された情報システムのメニューを利用できる。

【0026】今まで説明したように、本実施例を用いると情報処理システム管理部門では利用者のパスワード管理を行う必要があるが、一人一人の許可範囲についてまで関わる必要はなくなる。一人一人の許可範囲は組織の上位管理者およびその下の中間管理者が決めれば、必然的に下位者の範囲も決定されてくるので、許可範囲の誤りも少なくなる。このように本発明によれば企業における組織図に則ってセキュリティ管理の設定が容易にできるようになり、また下位者が組織図の範囲を超えてデータを利用することもできなくなり、情報処理システムの機密安全性が高められる。

【0027】

【発明の効果】本発明によれば、下位者の個人メニューをその上位者のメニューから作成することによって、情報システム管理部門の作業負担を軽減し、その部署に適合したセキュリティを設定することができるので、機密安全性が高まる。また、下位者は上位者の持つメニューを基にさらに制限したメニューからのみ情報システムに

8

アクセスするので機密安全性が高まる。また、担当者自身が上位者の持つメニューを基に許可された範囲から自分のメニューを作成、編集できるので情報システムを操作するときの操作性、視認性が高まる。また、人事異動によって担当者が別の部署に異動した場合でも、組織データを更新するだけで異動者の許可範囲を変更できるので、情報システム管理部門の作業負担を軽減でき、人事異動と許可範囲変更の時間差をなくすることができる。また、下位者の個人メニューをその上位者のメニューから作成する手段を備えたセキュリティ管理装置によって、情報システム管理部門の作業負担を軽減することができる。

【図面の簡単な説明】

【図1】本発明によるセキュリティ管理方法の一実施例を示す機能ブロック図である。

【図2】パスワードデータファイルの一例を示す構成図である。

【図3】個人メニューファイルの一例を示す構成図である。

【図4】組織データファイルの一例を示す構成図である。

【図5】本発明によるセキュリティ管理方法の一実施例を示すフローチャートである。

【図6】本発明によって作成された個人メニューの一実施例を示す画面である。

【図7】本発明によるセキュリティ管理方法において、担当者自身が自分のメニューを作成する場合の一実施例を示すフローチャートである。

【図8】本発明によるセキュリティ管理方法において、人事異動によって担当者が他部署に異動した場合の一実施例を示すフローチャートである。

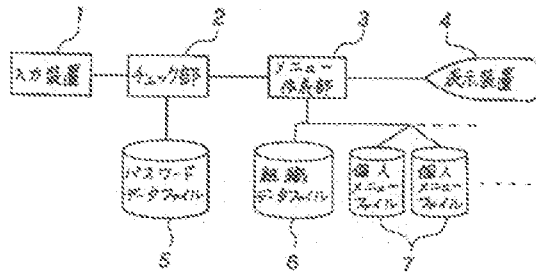
【図9】個人メニューを作成する操作の一実施例を示す画面である。

【図10】組織の階層に対応したメニューの一実施例を示す画面である。

【符号の説明】

- 1 入力装置
- 2 チェック部
- 3 メニュー作成部
- 4 表示装置
- 5 パスワードデータファイル
- 6 組織データファイル
- 7 個人メニューファイル

【 図1 】



【 図3 】

メニューコード	表示フラグ	表示名	起動プログラム名
MEN1	有	入力1	input.prg
MEN2	無	入力2	input2.prg
MEN3	有	出力1	output.prg
...

【 図6 】

メニュー : 経路情報システム	1
ログイン名 : kefirilm	社員コード : mgc101
管理レベル : 課長	部署 : 経理1課
1.日経費帳 2.部門別帳 3.期日管理帳 4.出納管理帳 5.予算管理帳 6.資金繰管理 7.照会印刷	

メニュー : 経路情報システム	1
ログイン名 : ktsrtoko	社員コード : wkc011
管理レベル : 担当	部署 : 経理1課
1.日経費帳 2.期日管理帳 3.出納管理帳	

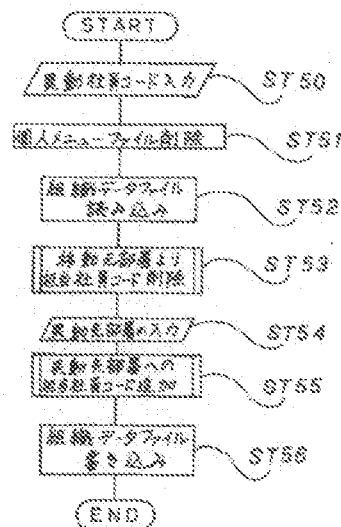
【 図2 】

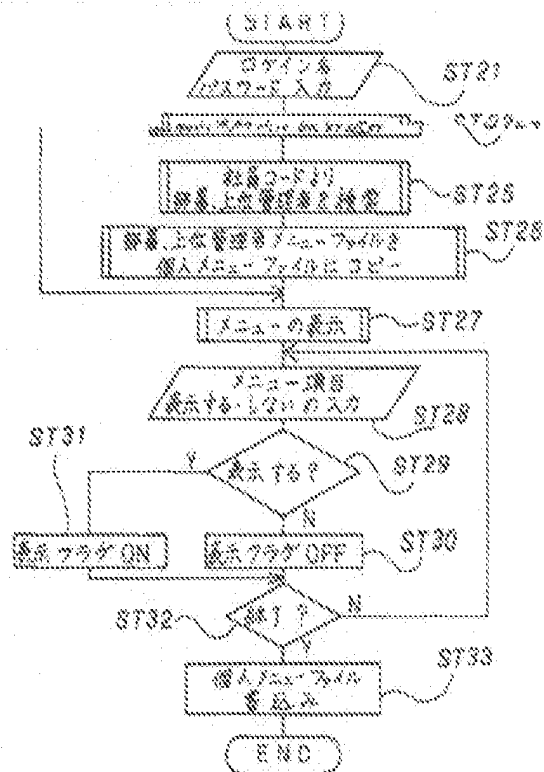
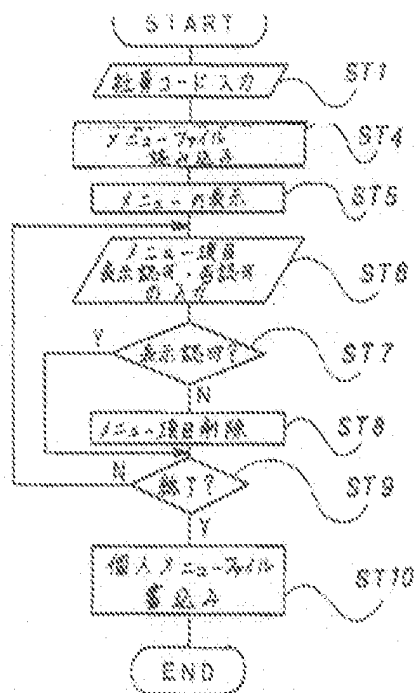
ログイン名	パスワード	社員コード	個人メニューファイル名
A	Password a	mgc 101	menu a
B	Password b	Wkc 011	menu b
C	Password c	Wkc 012	menu c
...

【 図4 】

部署コード	部署名	管理系 社員コード	経理系1 社員コード	経理系2 社員コード	...
AC 01	経理1課	mgc 101	wkc 010	wkc 011	...
AC 02	経理2課	mgc 301	wkc 031	wkc 032	...
...

【 図9 】





【 図10 】

101

メニュー : 新商品開発システム	
ログイン名: root	社員コード: superv
管理レベル: 全社	部署: 全社
1. 日常業務 2. 部門別業務 3. 項目別業務 4. 出納管理業務 5. 予算管理業務 6. 資金繰り業務 7. 経費分析 8. 明細管理 9. 財務管理 A. 売上管理 B. 予算管理 C. 経理決算処理 D. 給与管理 E. 退職金管理 F. 福利厚生 G. 給与計算 H. 給与支払 I. 給与振込 J. 給与明細 K. 給与計算	

102

メニュー : 新商品開発システム	
ログイン名: dpkehl	社員コード: dpm 101
管理レベル: 部	部署: 経理部
1. 日常業務 2. 部門別業務 3. 項目別業務 4. 出納管理業務 5. 予算管理業務 6. 資金繰り業務 7. 経費分析 8. 明細管理 9. 財務管理 A. 売上管理 B. 予算管理 C. 経理決算処理	

103

メニュー : 新商品開発システム	
ログイン名: ktanaka	社員コード: wkc 011
管理レベル: 担当	部署: 経理1課
1. 日常業務	

